Article 34 Amd't

09/402144

GR 97 P 1 - 1 - PCT/DE 98/00563

I claim as my Invention ~~New Patent Claims~~

420 Rec'd PCT/PTO 29 SEP 1999

a

Sub a9

1. Method for forming a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,

a) in which a segment checksum (PSi) is formed for each data segment (Di),

b) in which the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (PSi), and

c) in which the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation.

2. Method for checking a predetermined cryptographic commutative checksum which is allocated to digital data which are grouped into a number of data segments, by a computer,

a) in which the cryptographic commutative checksum is subjected to an inverse cryptographic operation to form a first cryptographic checksum (KP1),

b) in which a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z),

c) in which a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (PSj), and

d) in which the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

3. Method for forming and checking a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,

a) in which a segment checksum (PSi) is formed for each data segment (Di),

AMENDED SHEET

09402144 . 092599

Article 34 Amd't

a9 con't

b) in which the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (PSi),

c) in which the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation, a cryptographic commutative checksum being formed,

d) in which the cryptgographic commutative checksum (KP1) is subjected to an inverse cryptographic operation to form a first reconstructed cryptographic checksum (KP1),

e) in which a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z) of the digital data to which the first commutative checksum (KP1) is allocated,

f) in which a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (PSj), and

g) in which the second commutative checksum (KP2) is checked for a match with the first reconstructed commutative checksum (KP1).

4. Method according to one of Claims 1 to 3, in which the segment checksums (PSi, PSj) are formed in accordance with at least one of the following types:

- forming a hashing value,
- forming CRC codes,
- using at least one cryptographic one-way function.

5. Method according to one of Claims 1 to 4, in which the cryptographic operation is a symmetric cryptographic method.

6. Method according to one of Claims 1 to 4, in which the cryptographic operation is an asymmetric cryptographic method.

AMENDED SHEET

Article 34 Amend't

7. Method according to one of Claims 1 to 6, in which the commutative operation (⊕) exhibits the property of associativity.

8. Method according to one of Claims 1 to 7, in which digital data are protected, the data segments (Di) of which are not tied to an order.

9. Method according to one of Claims 1 to 7, in which digital data are protected which are processed in accordance with a network management protocol.

Sub a11

10. Arrangement for forming a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by means of an arithmetic and logic unit which is arranged in such a manner that

a) a segment checksum (PSi) is formed for each data segment (Di), and

b) the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (Psi), and

c) the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation.

11. Arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, by means of an arithmetic and logic unit which is arranged in such a manner that

a) the cryptographic commutative checksum is subjected to an inverse cryptographic operation to form a first cryptographic checksum (KP1),

b) a second segment checksum (Psj) is formed for each data segment (Dj, j = a .. z),

Article 34 Amd't

all amt

~~c) a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (PSj), and~~

~~d) the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).~~

~~12. Arrangement for forming and checking a first commutative checksum (KP1) for digital data which is grouped into a number of data segments (Di, i = 1 .. n), by means of at least one arithmetic and logic unit which is arranged in such a manner that~~

~~a) a segment checksum (PSi) is formed for each data segment (Di),~~

~~b) the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (Psi),~~

~~c) the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation, a cryptographic commutative checksum being formed,~~

~~d) the crystographic commutative checksum (KP1) is subjected to an inverse cryptographic operation to form a first reconstructed cryptographic checksum (KP1),~~

~~e) a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z) of the digital data to which the first commutative checksum (KP1) is allocated,~~

~~f) a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (Psj), and~~

~~g) the second commutative checksum (KP2) is checked for a match with the first reconstructed commutative checksum (KP1).~~

~~13.~~ a Arrangement according to one of Claims 10 to 12,

add a10 a12

AMENDED SHEET

Article 34 Amd't

in which the arithmetic and logic unit is arranged in such a manner that the segment checksums (PSi, PSj) are formed in accordance with at least one of the following types:

- forming a hashing value,
- forming CRC codes,
- using at least one cryptographic one-way function.

14. Arrangement according to one of Claims 10 to 13, in which the arithmetic and logic unit is arranged in such a manner that the cryptographic operation is a symmetric cryptographic method.

15. Arrangement according to one of Claims 10 to 13, in which the arithmetic and logic unit is arranged in such a manner that the cryptographic operation is an asymmetric cryptographic method.

16. Arrangement according to one of Claims 10 to 15, in which the arithmetic and logic unit is arranged in such a manner that the commutative operation (⊕) exhibits the property of associativity.

17. Arrangement according to one of Claims 10 to 16, in which the arithmetic and logic unit is set up in such a manner that the digital data are protected, the data segments (Di) of which are not tied to an order.

18. Arrangement according to one of Claims 10 to 16, in which the arithmetic and logic unit is arranged in such a manner that the digital data are protected which are processed in accordance with a network management protocol.